DEPARTMENT OF
HIGHER EDUCATION &
WORKFORCE DEVELOPMENT

COMPLIANCE UPDATE
By Kim Slote, Assistant Associate

ACTIVE RANSOMWARE CAMPAIGN!

On Sept. 1, 2020, the USDE published an Electronic Announcement: Technology Security Alert – Active Ransomware Campaign Targeting Education Institutions. Multiple ransomware attacks have been identified by Federal Student Aid. These attacks lead to denial of access to sensitive data and systems, unless a ransom is paid. Until an infection is completely remediated, ransomware can cripple an institution's ability to operate.

Several schools have reported that phishing attacks have been used to gain access to account credentials, which were then used to install and transmit ransomware across a network. Institutions are attractive targets, because of their privacy information, research data, financial information and intellectual property. To protect your institution, you are strongly encouraged to implement the following cybersecurity best practices recommended by FSA.

- *Establish a data backup process, ensure the backups are available and accessible, and store the backups offline*
- *Implement multi-factor authentication to mitigate account compromises*
- *Regularly patch hardware and software*
- *Continuously monitor institutional network to detect unauthorized access and malware*
- *Create and update your Incident Response Plan*
- *Ensure training resources emphasize phishing, as it is frequently the compromising entry point for ransomware attacks*

For more information on what your institution can do to protect itself, check out the Cybersecurity and Infrastructure Security Agency (CISA) information page on ransomware, located at https://www.us-cert.gov/Ransomware.

Report the incident immediately to cpssaig@ed.gov and FSASchoolCyberSafety@ed.gov, if you think your institution was targeted. Provide the following information in your email.

- *Name of the institution*
- *OPEID – School Code*

- *Date the incident occurred (if known)*
- *Date the incident was discovered*
- *Technical details of the ransomware (if known)*
- *Extent of the impact*
- *Remediation status (what has been done since discovery)*
- *Institution points of contact*

You should take the remediation steps below, if your institution falls victim to an attack.

- *Preemptively shut off network and systems to limit the spread of the ransomware*
- *Bring systems back up only after they have been checked and cleared of infection*
- *Block IP addresses that were related to the attack*
- *Force reset credentials for potentially affected accounts*
- *Perform forensic analysis on server, network, and application logs from recent weeks*
- *Restore data from backups*
- *Notify law enforcement of the criminal attack*

FSA will monitor the situation and will post additional information when appropriate.